ON PAGE 32

THE NEW YORK TIMES
19 December 1981

Excerpts From the Addre On Countering Russians

Special to The New York Times

WASHINGTON, Dec. 18 — Following are excerpts from the prepared text of a speech today by Attorney General William French Smith to the Los Angeles World Council on the threat of Soviet espionage:

President Reagan inherited an intelligence community that had been demoralized and debilitated by six years of public disclosures, denunciation, and — in addition — budgetary limitations.

Unfortunately, during this same period, our need for a reliable foreign intelligence capability was dramatically increasing. Communist takeovers in Indochina — as well as the loss of pro-Western governments in Central Asia, the Middle East, and the Horn of Africa — posed new dangers. By the time the Russians invaded Afghanistan and the Iranians took our diplomats hostage, the Carter Administration itself had begun to appreciate the need for more effective foreign intelligence.

The threat to our Government and its citizens from hostile intelligence services and international terrorist groups was also increasing dramatically.

Agents Seen in Various Guises

This threat, and particularly the activities of the K.G.B., have at long last received some media attention in recent months. I welcome this attention because it is important for the American public to realize that hostile intelligence agents increasingly operate in the United States under a number of guises:

First, as diplomats. About one-third of the Soviet bloc personnel in the United States assigned to embassies, consulates, and the U.N. or other international organizations are believed to be full-time intelligence officers. And over the last dozen years the number of official representatives of governments with hostile intelligence activities in our country has increased by 400 percent.

Second, as trading company representatives. There are dozens of corporations in the United States that are largely or exclusively owned by the Soviet bloc countries. Earlier this week in Los Angeles, a Polish trading company official who had been purchasing classified documents from an employee of one major defense contractor was sentenced to life in prison.

Third, as students, scientists, and reporters. Soviet bloc exchanges with the United States have increased dramatically over the past decade. And their ranks have been packed with full-time or parttime intelligence operatives.

Fourth, as immigrants and refugees. Although virtually nonexistent prior to 1973, Soviet immigration here has since then amounted to some 150,000. More recently, there has been a vast influx of Cuban refugees — who last year alone exceeded 100,000. We believe that a small but significant fraction of these recent refugees have been agents of Soviet and Cuban intelligence.

Finally, we know that hostile intelligence services continue to infiltrate agents under assumed identities. In 1980 the F.B.I. disclosed that Col. Rudolph Hermann of the K.G.B. had entered this country through Canada with his wife and son a dozen years earlier and had thereafter posed as a freelance photographer living in a suburb of New York City.

U.S. Agents Called Outnumbered

The likely number of foreign spies in our country in those guises has increased sharply over the last decade. Unfortunately, our resources have not increased. At one time the F.B.I. could match suspected hostile intelligence agents in the United States on a one-to-one basis. Now, the number of hostile agents has grown so much that our F.B.I. counterintelligence agents are greatly outnumbered.

In addition to increasing their number of agents, hostile intelligence services have placed a high priority on scientific and technical information, much of which is unclassified proprietary data. The "Silicon Valley" near San Francisco, and southern California defense contractors, for example, have been the targets of intensive foreign intelligence efforts.

Foreign intelligence agents — often posing as businessmen, diplomats, or newsmen — befriend employees in the United States, request innocuous information on various pretexts with nominal reimbursement, and finally attempt to obtain sensitive information in return for substantial cash payments. In a case last year, a Belgian businessman was charged with offering up to $500,000 to American employees to steal computer software technology he was seeking for the Soviets.

United States businessmen traveling in the Soviet bloc are lured into compromising situations and then blackmailed into providing information and services.

Switzerland. Earlier this month in Los Angeles, a Federal court sentenced two individuals to prison for illegally exporting state-of-the-art computers and other technological equipment to West Germany for diversion to Soviet bloc countries.

The costs to national security are incalculable because we depend upon our superior technology as a defense against Soviet military advantages in manpower and sheer volume of weaponry. A television documentary on the K.G.B. shown by the Canadian Broadcasting Company a few months ago, for example, concluded that the theft of inertial guidance technology by Soviet intelligence improved the accuracy of Soviet ICBM's and made U.S. land-based missiles vulnerable — and argued that the theft created the need to build a costly MX missile system as a replacement. The multibillion-dollar cost of the proposed MX missile system may thus illustrate the effectiveness of Soviet intelligence.

Perhaps even more insidious is the threat posed by hostile "active measures" in this country, which are aimed at influencing public opinion and the political process through "disinformation" and "agents of influence." Most serious of all, however, is the threat of international terrorism. Although we have been fortunate as a country to have been spared the degree of terrorism experienced by many of our Western European allies, we cannot permit our relative good luck to engender complacency.

A small number of well-trained fanatics could change our fortunes overnight. As all of you know from press reports, the threat is real today. Libya's capability of sponsoring an effort to assassinate high U.S. Government officials provides a sobering example. As members of an open society that is the target of aggressive foreign powers, we must all recognize the grave threat from hostile intelligence and the need for more effective U.S. intelligence and counterintelligence. But we must do more than merely recognize such paramount concerns.

CONTINUED

The Reagan Administration is firmly committed to revitalizing the United States intelligence effort. That commitment is apparent in the President's recent promulgation of three new Executive Orders:

Executive Order 12331 re-established the President's Foreign Intelligence Advisory Board;

Executive Order 12333, signed two weeks ago, clarifies the authorities, responsibilities, and limitations concerning U.S. intelligence; and

Executive Order 12334 continues the President's Intelligence Oversight Board.

Stepping Up Resources

Revised procedures and guidelines will implement the new Executive Orders. This Administration is also making available increased resources to the intelligence community and supports rebuilding personnel levels.

On behalf of the Administration, the Justice Department has proposed amendments to the Freedom of Information Act to improve our ability to protect intelligence sources and methods. In addition, we support exemption of C.I.A. and other key intelligence agencies from the requirements of that Act.

The Administration also supports new legislation that would impose criminal penalties on those who make a practice of ferreting out and exposing the classified identities of our intelligence agents — frequently risking lives as well as our security interests.

Finally, the Justice Department is committed to vigorous enforcement of national security legislation, including laws prohibiting unlawful export of advanced technology and munitions.

Throughout, however, our goal has been to improve the effectiveness of U.S. intelligence agencies without endangering the rights of Americans. Intelligence activities must be conducted in a lawful manner. We will maintain five basic safeguards to insure that they are: first, strict observance of Fourth Amendment and statutory requirements governing searches and electronic surveillance; second, a thorough appreciation for the legal distinctions between foreign intelligence and domestic security matters; third, appropriate limitations on the authority of the C.I.A. to function within the United States; fourth, cooperation with Congressional oversight through the House and Senate intelligence committees; and fifth, effective oversight within the Executive branch itself by the President's Intelligence Oversight Board and by the Attorney General as chief law enforcement officer of the United States.

First, the Fourth Amendment protects all persons within the territorial jurisdiction of the United States, including aliens and commercial enterprises. It also protects Americans when they are abroad. Those protections, which generally require issuance of a judicial warrant, apply to the so-called "Fourth Amendment techniques" — searches and seizures, wiretapping, bugging, and closed-circuit monitoring. The courts have held that other types of surveillance in public places, including "shadowing" or photographing, do not constitute Fourth Amendment techniques.

Although the issue has not been decided by the Supreme Court, the U.S. Courts of Appeals have held that the use of Fourth Amendment techniques for foreign intelligence purposes does not require a judicial warrant. Instead, the courts have determined that the President may approve the use of such techniques as an exercise of his constitutional authority as Commander in Chief and principal executor of our country's foreigh policy. This Presidential authority has been delegated to the Attorney General, who may approve proposed activities based upon a finding in each case that the target of the activity is an "agent of a foreign power."

Judges Supplementing Act

The constitutional requirements governing electronic surveillance for foreign intelligence purposes within the United States have themselves been supplemented by the Foreign Intelligence Surveillance Act of 1978. Under this Act, a special court of Federal district judges considers Government applications to conduct electronic surveillance within this country for foreign intelligence purposes. All such applications must first be approved by the Attorney General.

Second, in addition to those Fourth Amendment and statutory safeguards, there are also limits on the purposes for which intelligence activities may be undertaken. In the 1960's and early 1970's, efforts to gather information and affect the activities of domestic dissident groups were blended with foreign intelligence and counterintelligence activities under the blanket of "national security." In addition, intelligence agencies sometimes became involved in politically motivated spying on domestic groups.

In its landmark decision in the "Keith" case, the U.S. Supreme Court in 1972 held that the Executive could not use its constitutionally based national security powers to justify surveillance of purely domestic dissident groups. Where there is no foreign connection, efforts to counter domestic unrest must be conducted in accordance with the standards applicable to other law-enforcement activities, including the warrant requirement. Today, domestic security investigations are conducted in a manner that is both administratively and legally separated from foreign intelligence and counterintelligence activities.

The functions and activities of the intelligence agencies are thus focused on foreign persons and events abroad, not U.S. citizens or businesses.